



April 27, 2018

CPT ID: <<ID>>
<EmployeeName>
<Address>
<City>, <State> <Zip>

NOTICE OF DATA BREACH

Dear <FullName>:

CPT Group Inc. (“CPT”) understands the importance of protecting the information it maintains. Regrettably, we write to inform you of a recent incident that may have involved your personal information, which was provided to CPT in connection with the <<CaseName>> class action settlement. This notice explains the incident, measures we have taken, and some steps you can take in response.

What Happened

CPT is a class action settlement administrator. We send settlement notices to class members, answer questions class members may have, and process settlement payments. To accomplish this function, we are provided with necessary data about class members, including certain types of personal information.

On February 8, 2018, CPT learned through its ongoing forensics investigation of a phishing email incident that certain emails and attachments could have potentially been accessed by an unauthorized person. The investigation, conducted with the assistance of a computer forensics firm, determined that an unknown individual had access to a CPT employee’s email account from November 22, 2017 through December 8, 2017. While some of the attachments were encrypted and/or password protected spreadsheets, CPT could not rule out the possibility that the spreadsheet passwords may have also been available to the attacker. Although, to date, we do not know that any of your sensitive personal information was accessed without permission, we are providing you this notification out of an abundance of caution.

What Information Was Involved

The information that could have been accessed in the affected employee’s account includes your name, address, and Social Security number.

What We Are Doing

CPT regrets that this incident occurred. In addition to providing you notice of the incident, CPT has taken substantial steps to enhance its existing network and email security, including implementing multi-factor authentication, and is re-educating and training its employees to help prevent a similar incident from happening in the future.

What You Can Do

We encourage you to remain vigilant by reviewing your account statements for any unauthorized activity. You should also review the additional information on the following pages on ways to protect yourself. We have arranged for Kroll to provide identity monitoring at no cost to you for one year. Kroll is a global leader in risk mitigation and response, and their team has extensive experience helping people who have sustained an unintentional exposure of confidential data. Your identity monitoring services include Credit Monitoring, Fraud Consultation, and Identity Theft Restoration. For more information on identity theft prevention and Kroll Credit Monitoring, including instructions on how to activate your complimentary one-year membership, please visit the below website.

Visit **my.idmonitoringservice.com** to activate and take advantage of your identity monitoring services.

*You have until **July 26, 2018** to activate your identity monitoring services.*

Membership Number: <<MonitoringCode>>

For More Information

We apologize for any inconvenience caused by this incident. If you have questions about this incident or the recommended next steps, please call toll-free 1-833-219-9086 Monday through Friday between 8:00 am and 5:30 pm, Pacific Time.

Sincerely,



Julie Green
Senior V.P. of Operations
CPT Group, Inc.



TAKE ADVANTAGE OF YOUR IDENTITY MONITORING SERVICES

You've been provided with access to the following services¹ from Kroll:

Single Bureau Credit Monitoring

You will receive alerts when there are changes to your credit data—for instance, when a new line of credit is applied for in your name. If you do not recognize the activity, you'll have the option to call a Kroll fraud specialist, who can help you determine if it's an indicator of identity theft.

Fraud Consultation

You have unlimited access to consultation with a Kroll fraud specialist. Support includes showing you the most effective ways to protect your identity, explaining your rights and protections under the law, assistance with fraud alerts, and interpreting how personal information is accessed and used, including investigating suspicious activity that could be tied to an identity theft event.

Identity Theft Restoration

If you become a victim of identity theft, an experienced Kroll licensed investigator will work on your behalf to resolve related issues. You will have access to a dedicated investigator who understands your issues and can do most of the work for you. Your investigator can dig deep to uncover the scope of the identity theft, and then work to resolve it.

¹ Kroll's activation website is only compatible with the current version or one version earlier of Internet Explorer, Chrome, Firefox, and Safari. To receive credit services, you must be over the age of 18 and have established credit in the U.S., have a Social Security number in your name, and have a U.S. residential address associated with your credit file.

MORE INFORMATION ON WAYS TO PROTECT YOURSELF

Even if you choose not to take advantage of this free credit monitoring, we recommend that you remain vigilant for incidents of fraud or identity theft by reviewing your account statements and free credit reports for any unauthorized activity. You may obtain a copy of your credit report, free of charge, once every 12 months from each of the three nationwide credit reporting companies. To order your annual free credit report, please visit www.annualcreditreport.com or call toll free at 1-877-322-8228. Contact information for the three nationwide credit reporting companies is as follows:

Equifax, PO Box 740241, Atlanta, GA 30374, www.equifax.com, 1-800-685-1111

Experian, PO Box 2002, Allen, TX 75013, www.experian.com, 1-888-397-3742

TransUnion, PO Box 2000, Chester, PA 19016, www.transunion.com, 1-800-916-8800

If you believe you are the victim of identity theft or have reason to believe your personal information has been misused, you should immediately contact the Federal Trade Commission and/or the Attorney General's office in your state. You can obtain information from these sources about steps an individual can take to avoid identity theft as well as information about fraud alerts and security freezes. You should also contact your local law enforcement authorities and file a police report. Obtain a copy of the police report in case you are asked to provide copies to creditors to correct your records. Contact information for the Federal Trade Commission is as follows:

Federal Trade Commission, Consumer Response Center, 600 Pennsylvania Avenue, NW
Washington, DC 20580, 1-877-IDTHEFT (438-4338), www.ftc.gov/idtheft